Advances in Cryptology, ASIACRYPT 2004: 10th International ... - Google Books Result
by Pil Joong Lee - 2004 - Computers - 546 pages
[15], all previous undeniable **signatures** were based on the discrete ... 2 The **Group Homomorphism** Interpolation Problem 2.1 Problem Definitions Given two ...
books.google.com/books?isbn=3540239758...

Thèse EPFL 3691 (2006) Jean Monnerat
On the other hand, by selecting **group homomorphisms** with a small **group** range, we obtain very short **signatures**. After providing theoretical results related ...
library.epfl.ch/theses/?nr=3691 - 37k - Cached - Similar pages

LNCS 3329 - Generic Homomorphic Undeniable **Signatures**
the sense that we transform a private **group homomorphism** from public. groups G to H (the order of H being public) into an undeniable **signature**. scheme. ...
www.springerlink.com/index/480K2P4L7GJB9ALX.pdf - Similar pages

> Verifiable Encryption, **Group** Encryption, and Their Applications to ...
> knows a **signature** on given message reduces to demonstrating that one knows. a pre-image under a **group homomorphism**. This is true for any of the standard ...
> www.springerlink.com/index/BVXEU179UFUEHJVV.pdf - Similar pages
> [More results from www.springerlink.com]

[PDF] Generic Homomorphic Undeniable **Signatures**
File Format: PDF/Adobe Acrobat - View as HTML
Interpolation of **Group Homomorphisms**. Our **Signature** Scheme. Conclusion. Generic Homomorphic Undeniable **Signatures**. J. Monnerat. S. Vaudenay ...
www.iris.re.kr/ac04/data/Asiacrypt2004/09%20Digital%20**Signatures**/01_Jean%20Monnerat.pdf - Similar pages

[PDF] Short undeniable **SignatureS**: deSign, analySiS, and applicationS
File Format: PDF/Adobe Acrobat - View as HTML
group homomorphism which he keeps secret. Based on these protocols, we devise. our new undeniable **signature** scheme and prove its security in a formal way. ...
biblion.epfl.ch/EPFL/theses/2006/3691/3691_abs.pdf - Similar pages

[PDF] How to Sign with One Bit
File Format: PDF/Adobe Acrobat - View as HTML
1-bit **signature**. We introduce a new computational problem related to the interpolation of. **group homomorphisms**. Many famous cryptographic problems including ...
lasecwww.epfl.ch/pub/lasec/doc/MV04b.pdf - Similar pages

> LASEC
> If there exist several **group homomorphisms**, then the signer can change it and deny his **signatures**. Since this violates one of the security requirements, ...
> lasecwww.epfl.ch/memo/memo_mova.shtml - 46k - Cached - Similar pages
> [More results from lasecwww.epfl.ch]

(WO/2005/081451) METHOD TO GENERATE, VERIFY AND DENY AN UNDENIABLE ...

The method according to claim 2, wherein the **group homomorphism** (f) computation is ...

A Method of confirming by a Verifier an undeniable **signature** (y1, ...
www.wipo.int/pctdb/en/wo.jsp?IA=EP2005001335&DISPLAY=CLAIMS - 28k -
Cached - Similar pages

Method to generate, verify and deny an undeniable **signature ...**
[0214] The above described **group homomorphism** of the undeniable **signature** scheme is in the context of characters to hard characters, which means a ...
www.freepatentsonline.com/20050193048.html - 68k - Cached - Similar pages

1 2 3 4 5 6 7 8 9 10 **Next**

---

group homomorphism signatures Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---